(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 780 797**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 08532**

(51) Int Cl[7] : G 06 F 12/14, H 04 L 9/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 03.07.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 07.01.00 Bulletin 00/01.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *BONNET GERARD* — FR et *FRANCOIS PAUL* — FR.

(72) **Inventeur(s)** : BONNET GERARD et FRANCOIS PAUL.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : RINUY SANTARELLI.

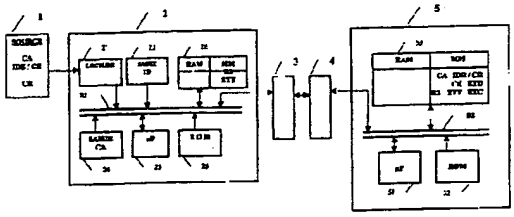
(54) DISPOSITIF ET PROCEDE D'AUTHENTIFICATION.

(57) L'invention concerne l'authentification d'un utilisateur, utilisant une source de données propres à l'utilisateur, et deux dispositifs de traitement.

Le premier dispositif forme deux identificateurs morphologiques (ID1, ID2), lit dans la source (1) un premier identificateur de référence (IDE/ CE) codé par une première clé de codage (CE), et une seconde clé de codage (CR), et transmet le second identificateur morphologique (ID2) et la seconde clé (CR) au second dispositif (5).

Celui-ci code le second identificateur morphologique (ID2) par la seconde clé (CR), puis compare le résultat avec un second identificateur de référence (IDR/ CR) codé par la seconde clé et, si il y a identité, transmet une table de codage (TCE), vers le premier dispositif (2).

Ce dernier code le premier identificateur morphologique (ID1) par table de codage (TCE), puis compare le résultat avec le premier identificateur de référence (IDE/ CE) codé par la première clé de codage.



FR 2 780 797 - A1

La présente invention concerne de manière générale l'authentification d'un utilisateur pour déterminer s'il est autorisé à effectuer une opération prédéterminée.

Afin de fixer les idées, on définit ici des termes qui seront utilisés dans la suite :

- utilisateur : personne susceptible d'effectuer une opération prédéterminée, telle qu'accès à un serveur informatique, retrait d'argent dans une banque, transaction commerciale, accès à un local ou un véhicule, par exemple.

- identificateur : tout nom, caractère ou code qui caractérise une donnée et permet de la reconnaître au cours d'une authentification.

- table de codage : ensemble ordonné de mots, chaque mot étant une suite ordonnée de caractères issus d'un ensemble de caractères. Une table de codage est utilisée pour crypter, de manière classique, des données.

- clé de codage : indicateur ou adresse d'une table de codage dans un ensemble ordonné de tables de codage.

- authentification : série d'opérations visant à s'assurer de l'identité d'un utilisateur pour déterminer s'il est habilité à effectuer une opération.

De nombreuses techniques d'authentification sont connues et utilisées afin de réserver la possibilité d'effectuer une opération prédéterminée à une personne. Ces techniques ont comme point commun d'échanger des données entre un premier dispositif à la disposition de l'utilisateur et un second dispositif, généralement distant, tel qu'un ordinateur central de traitement. Par

exemple, un utilisateur fournit un mot de passe pour accéder à un serveur informatique, ou fournit le numéro de sa carte bancaire et sa signature manuscrite pour régler un achat effectué par correspondance. Le mot de passe, ou le numéro de carte bancaire et la signature de l'utilisateur constituent des identificateurs.

Cependant, le risque d'utilisation frauduleuse est élevé. En effet, en cas de perte ou de vol d'un tel identificateur, une autre personne peut l'utiliser pour effectuer l'opération correspondante.

Pour réduire ce risque, des identificateurs morphologiques sont maintenant utilisés. Par exemple, l'utilisateur doit fournir ses empreintes digitales qui sont numérisées et codées pour fournir un mot numérique qui sert d'identificateur morphologique pour une opération donnée.

L'identificateur morphologique est alors mémorisé soit dans le premier dispositif, soit dans le second dispositif, soit encore dans les deux dispositifs. Il est alors possible de copier de manière frauduleuse cet identificateur, et par conséquent de l'utiliser ensuite. En outre, dans le cas où la reconnaissance de l'identificateur est réalisée par le second dispositif, ce dernier envoie un signal d'authentification au premier dispositif. Ce signal peut être copié et ensuite fourni de manière frauduleuse à ce premier dispositif.

Pour résoudre ces problèmes, il a été envisagé de rendre plus complexe le codage de l'identificateur et/ou le codage des données transmises entre les deux dispositifs. De nouvelles techniques d'identification morphologiques ont également été envisagées.

Néanmoins, les techniques connues ne permettent pas une authentification suffisamment fiable, c'est-à-dire insensible à un grand nombre de possibilités de fraudes, pour déterminer si un utilisateur est habilité à effectuer une opération.

La présente invention vise à remédier aux inconvénients de la technique antérieure, en fournissant un procédé d'authentification d'un utilisateur, utilisant une source de données propres à l'utilisateur, et un premier et un second dispositifs de traitement,

caractérisé en ce qu'il comporte les étapes de :

- formation d'un premier et d'un second identificateurs morphologiques, par le premier dispositif,

- lecture d'un premier identificateur de référence codé par une première clé de codage, mémorisé dans la source de données, par le premier dispositif,

- lecture d'une seconde clé de codage mémorisée dans la source de données, par le premier dispositif,

- transmission du second identificateur morphologique et de la seconde clé de codage au second dispositif,

- codage du second identificateur morphologique par la seconde clé de codage, par le second dispositif,

- comparaison, par le second dispositif, du second identificateur morphologique codé par la seconde clé de codage avec un second identificateur de référence codé par la seconde clé de codage et mémorisé dans le second dispositif et, si il y a identité,

- transmission d'une première table de codage, mémorisée dans le second dispositif, vers le premier dispositif,

- codage du premier identificateur morphologique au moyen de la première table de codage, par le premier dispositif,

- comparaison, par le premier dispositif, du premier identificateur morphologique codé au moyen de la première table de codage avec le premier identificateur de référence codé par la première clé de codage.

Grâce au procédé selon l'invention, l'authentification d'un utilisateur est fiabilisée.

L'invention utilise deux identificateurs morphologiques, chacun étant traité dans l'un ou l'autre des dispositifs, ce qui sécurise le traitement.

En outre, l'invention utilise deux identificateurs de référence, en association respective avec deux clés de codage. Aucun identificateur de référence n'est mémorisé avec sa clé de codage.

Il est à noter que le volume de données échangées entre les deux dispositifs est faible, le débit et le temps de transmission sont ainsi réduits, et le traitement d'authentification est rapide.

Selon une caractéristique préférée, l'étape de formation comporte la lecture d'un identificateur morphologique initial puis le partage de l'identificateur morphologique initial en les premier et second identificateurs morphologiques.

Selon une autre caractéristique préférée, l'étape de transmission du second identificateur morphologique et de la seconde clé de codage au second dispositif comporte la sélection d'une première table de codage de transmission dans un ensemble de table de codage de transmission, le codage du second identificateur morphologique et de la seconde clé de codage par la première table de codage de transmission, et la transmission du second identificateur morphologique et de la seconde clé de codage codés par la première table de codage de transmission.

Ainsi, la transmission est cryptée, ce qui limite les risques de fraudes.

Selon une caractéristique préférée, liée à la précédente, l'étape de décodage, par le second dispositif, du second identificateur morphologique et de la seconde clé de codage codés par la première table de codage de transmission, préalablement à l'étape de codage du second identificateur morphologique par la seconde clé de codage.

Selon une caractéristique préférée, le procédé comporte en outre la lecture d'une clé alphanumérique, mémorisée dans la source de données, par le premier dispositif, et la transmission de la clé alphanumérique au second dispositif.

Selon une autre caractéristique préférée, le procédé comporte le codage, par le premier dispositif, de la clé alphanumérique par la première table de codage de transmission, préalablement à sa transmission.

Selon une autre caractéristique préférée liée à la précédente, le procédé comporte le décodage, par le second dispositif, de la clé alphanumérique codée par la première table de codage de transmission.

La clé alphanumérique permet d'accéder à un ensemble de table de codage mémorisé dans le second dispositif, et la seconde clé de codage permet de trouver une seconde table de codage dans cet ensemble de codage.

La clé alphanumérique permet d'accéder au second identificateur de référence codé par la seconde clé de codage, mémorisé dans le second dispositif.

Selon une autre caractéristique préférée, la transmission de la première table de codage comporte le codage préalable, par le second dispositif, de la première table de codage par une seconde table de codage de transmission.

Cette transmission est également cryptée, ce qui limite les risques de fraude.

Selon une autre caractéristique préférée, liée à la précédente, le procédé comporte le décodage, par le premier dispositif, de la première table de codage codée par la seconde table de codage de transmission, préalablement au codage du premier identificateur morphologique au moyen de la première table de codage.

Corrélativement, l'invention concerne un système d'authentification d'un utilisateur, comportant une source de données propres à l'utilisateur, et un premier et un second dispositifs de traitement,

caractérisé en ce que le premier dispositif comporte :

- des moyens de formation d'un premier et d'un second identificateurs morphologiques,

- des moyens de lecture d'un premier identificateur de référence codé par une première clé de codage, mémorisé dans la source de données,

- des moyens de lecture d'une seconde clé de codage mémorisée dans la source de données,

- des moyens de transmission du second identificateur morphologique et de la seconde clé de codage au second dispositif,

en ce que le second dispositif comporte :

- des moyens de codage du second identificateur morphologique par la seconde clé de codage,

- des moyens de comparaison du second identificateur morphologique codé par la seconde clé de codage avec un second

identificateur de référence codé par la seconde clé de codage et mémorisé dans le second dispositif, et,

- des moyens de transmission, si il y a identité, d'une première table de codage, mémorisée dans le second dispositif, vers le premier dispositif,

et en ce que le premier dispositif comporte :

- des moyens de codage du premier identificateur morphologique (ID1) au moyen de la première table de codage,

- des moyens de comparaison du premier identificateur morphologique codé au moyen de la première table de codage avec le premier identificateur de référence codé par la première clé de codage.

L'invention concerne encore le premier dispositif ainsi que le second dispositif, comportant les caractéristiques précédentes.

Le système d'authentification, le premier et le second dispositifs comportent des moyens de mise en œuvre du procédé exposé ci-dessus.

Les avantages du système d'authentification, du premier et du second dispositifs sont analogues à ceux du procédé précédemment exposés.

Les caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture d'un mode préféré de réalisation illustré par les dessins ci-joints, dans lesquels :

- la figure 1 représente de manière schématique un système d'authentification d'utilisateur selon un mode de réalisation de la présente invention,

- les figures 2 à 4 représentent un algorithme d'authentification selon un mode de réalisation de l'invention.

Selon le mode de réalisation choisi et représenté à la **figure 1**, un système pour authentifier un utilisateur pour déterminer s'il est autorisé à effectuer une opération prédéterminée comporte une source 1 de données d'identification propres à un utilisateur particulier. La source 1 est par exemple une carte à puce, ou une carte magnétique, ou encore un chèque magnétique.

Les données d'identification mémorisées dans la source 1 sont :

- une clé alphanumérique CA propre à l'utilisateur.

- un premier identificateur de référence IDE/CE codé par une première clé de codage CE, l'identificateur de référence IDE étant propre à l'utilisateur et la clé de codage CE étant attribuée à l'utilisateur. Le premier identificateur de référence IDE/CE codé par une première clé de codage CE est le premier identificateur de référence IDE qui a été crypté par une table de codage TCE repérée par son adresse, ou clé de codage, CE dans un ensemble de table de codage.

- une seconde clé de codage CR attribuée à l'utilisateur.

De manière générale, on appellera ici "données codées par une clé" des données cryptées par une table de codage ayant cette clé comme adresse dans un ensemble.

La source 1 comporte une sortie reliée à un premier dispositif 2 de traitement et codage selon l'invention. Le dispositif 2 comporte un bus de données B1 auquel sont reliés les circuits suivants :

- un circuit 21 de lecture des données mémorisées dans la source 1. Le circuit 21 est par exemple un lecteur de carte à puce, ou un lecteur de carte magnétique ou de chèque magnétique.

- un terminal 22 de saisie d'identificateur morphologique ID, par exemple un terminal de prise d'empreintes digitales.

- un terminal 24 de saisie de clé alphanumérique CA, dans le cas où cette clé alphanumérique n'est pas mémorisée dans la source 1. Le terminal 24 est facultatif.

- un premier circuit de traitement et codage 23. Le circuit 23 est par exemple réalisé au moyen d'un microprocesseur.

- une mémoire morte (ROM) 25 dans laquelle est mémorisé un programme de traitement et de codage qui sera décrit dans la suite.

- une mémoire 26.

La mémoire 26 comporte une mémoire vive (RAM) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution dudit programme.

La mémoire 26 comporte par exemple un disque dur pour mémoriser des données fixes, qui sont les suivantes.

La mémoire 26 mémorise un ensemble ETT de tables de codage de transmission T_1 à T_N, où N est un entier. Ces tables sont associées au couple de dispositifs 2 et 5 et sont utilisées pour crypter, de manière aléatoire, les transmissions de données entre les deux dispositifs, comme il apparaîtra dans la suite.

La mémoire 26 mémorise également une référence R2 relative au dispositif 2 considéré.

Un premier circuit d'émission/réception 3, comportant par exemple un modem, est également relié au bus B1. Le circuit 3 est intégré au dispositif 2, ou est relié à ce dernier. Le circuit 3 échange des données avec un second circuit d'émission/réception 4 généralement distant, via un support de transmission qui peut être le réseau téléphonique commuté, ou une ligne spécialisée, ou encore un faisceau hertzien. Les circuits 3 et 4 effectuent des opérations classiques de détection et correction d'erreur, qui ne seront pas décrites ici.

Le circuit d'émission/réception 4 fait partie d'un second dispositif de traitement et codage 5 selon l'invention, ou le circuit 4 est relié au dispositif 5. Les dispositifs 2 et 5 échangent des données via les circuits 3 et 4. Les dispositifs 2 et 5 peuvent être uniquement destinés à échanger des données d'authentification, ou en variante être des sous-ensembles de dispositifs connus en soi. Selon les applications, un dispositif 2 donné est associé à un dispositif 5 donné, ou une pluralité de dispositifs 2 est associée à un dispositif 5 donnée. Par exemple, une pluralité d'utilisateurs est susceptible d'utiliser les dispositifs 2, qui communiquent avec un dispositif 5.

Le dispositif 5 comporte un bus de données B2 auquel sont reliés les circuits suivants :

- un second circuit de traitement et codage 51. Le circuit 51 est par exemple réalisé au moyen d'un microprocesseur.

- une mémoire morte (ROM) 52 dans laquelle est mémorisé un programme de traitement et de codage qui sera décrit dans la suite.

- une mémoire 53.

La mémoire 53 comporte une mémoire vive (RAM) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution dudit programme.

La mémoire 53 comporte également un disque dur, par exemple, pour mémoriser des données fixes appartenant trois catégories de données :

La première catégorie est un ensemble ETC de tables de codage. Chaque table de codage a une adresse dans l'ensemble ETC.

La deuxième catégorie comporte des paramètres relatifs à chacun des dispositifs 2 susceptibles de communiquer avec le dispositif 5 :

- la référence R2 relative à chacun des dispositifs 2, pour identifier ce dispositif.

- l'ensemble ETT des tables de codage de transmission T_1 à T_N. L'ensemble ETT est propre au couple considéré de dispositifs 2 et 5. Cet ensemble comporte les adresses des tables T_1 à T_N dans l'ensemble ETC, ou en variante comporte les tables T_1 à T_N.

La troisième catégorie comporte des paramètres relatifs à chacun des utilisateurs susceptibles de procéder à une authentification selon la présente invention :

- l'ensemble des clés alphanumériques CA respectivement associées aux utilisateurs habilités à effectuer l'opération prédéterminée.

- un ensemble de seconds identificateurs de référence IDR/CR respectivement associés aux utilisateurs autorisés à effectuer l'opération et codés par les secondes clés de codage CR. Un identificateur de référence IDR est propre à un utilisateur et une clé de codage CR est attribuée à chaque utilisateur. Le second identificateur de référence IDR/CR codé par le seconde clé de codage CR est le second identificateur de référence IDR qui a été crypté par une table de codage TCR repérée par son adresse, ou clé de codage, CR dans un ensemble de table de codage.

- l'ensemble des premières clés de codage CE respectivement associées aux utilisateurs habilités à effectuer l'opération.

- un ensemble ETU de tables de codage utilisateur. Les tables de codage utilisateur sont propres au couple utilisateur-dispositif 5. L'ensemble ETU comporte les adresses des tables TCE dans l'ensemble ETC, ou en variante comporte les tables. Une table TCE a pour adresse dans l'ensemble ETU une première clé de codage CE.

Pour mettre en œuvre l'invention, le premier dispositif forme deux identificateurs morphologiques ID1, ID2, lit dans la source de données 1 un premier identificateur de référence IDE/CE codé par une première clé de codage CE, et une seconde clé de codage CR, et transmet le second identificateur morphologique ID2 et la seconde clé de codage CR au second dispositif 5.

Celui-ci code le second identificateur morphologique ID2 par la seconde clé de codage CR, puis compare le résultat avec un second identificateur de référence IDR/CR codé par la seconde clé de codage et, si il y a identité, transmet une première table de codage TCE, vers le premier dispositif 2.

Ce dernier code le premier identificateur morphologique ID1 au moyen de la première table de codage TCE, puis compare le résultat avec le premier identificateur de référence IDE/CE codé par la première clé de codage.

Le fonctionnement du système de la figure 1 est maintenant décrit en détail au moyen de trois organigrammes représentés aux figures 2, 3 et 4.

L'organigramme de la **figure 2** comporte des étapes E1 à E5 mémorisées en mémoire 25, qui décrivent le fonctionnement du premier dispositif 2 de traitement et codage lorsqu'un utilisateur effectue l'opération propre à faire lire les données de la source 1 par le circuit de lecture 21, par exemple en introduisant sa carte à puce dans le lecteur approprié.

Ce premier traitement consiste globalement à transmettre un identificateur morphologique, dit second identificateur morphologique, vers le second dispositif 5.

L'étape E1 est la lecture dans la source 1 par le circuit 21 de la clé alphanumérique CA, de l'identificateur de référence IDE/CE codé par la

première clé de codage CE, et de la seconde clé de codage CR, et la mémorisation de ces paramètres en mémoire 26.

En variante, l'utilisateur saisit en outre la clé alphanumérique CA sur le terminal 24.

L'étape suivante E2 est la lecture de l'identificateur morphologique ID par le circuit 22. Le circuit 22 est par exemple un circuit de prise d'empreintes digitales, qui sont codées sous la forme d'un mot numérique. Ce mot constitue l'identificateur morphologique ID et est mémorisé en mémoire 26.

L'étape suivante E3 est le partage de l'identificateur morphologique ID en deux identificateurs morphologiques ID1 et ID2. L'identificateur morphologique ID est un mot numérique de longueur prédéterminée. Le partage consiste par exemple à couper le mot numérique en deux mots de longueur prédéterminée. Comme il apparaîtra dans la suite, l'identificateur morphologique ID1 sera à comparer avec l'identificateur de référence IDE, et l'identificateur morphologique ID2 sera à comparer avec l'identificateur de référence IDR.

En variante, les étapes E2 et E3 sont remplacées par la lecture de deux identificateurs morphologiques distincts qui seront à comparer respectivement avec l'identificateur de référence IDE et l'identificateur de référence IDR.

Dans tous les cas, les identificateurs de référence sont déterminés lors d'une initialisation au cours de laquelle les identificateurs morphologiques, soit issus du partage d'un identificateur morphologique, soit distincts, sont déterminés et mémorisés en tant qu'identificateurs de référence.

L'étape suivante E4 est la sélection aléatoire d'une table de codage T_n parmi l'ensemble ETT de tables de codage de transmission mémorisé en mémoire 26, où n est un entier compris entre 1 et N. La sélection de la table T_n est suivie par le codage de la clé alphanumérique CA, du second identificateur morphologique ID2 formé à l'étape précédente et de la clé de codage CR au moyen de la table de codage T_n. Ce codage est un cryptage classique des données par le ou les mot(s) de la table de codage.

L'étape suivante E5 est la transmission des données codées à l'étape E4, d'un indicateur IN_n représentatif de la table T_n sélectionnée à l'étape E4, et de la référence R2 du dispositif 2 vers le second dispositif 5, au moyen du circuit 3.

La **figure 3** représente les opérations effectuées par le dispositif 5 lorsqu'il reçoit des données depuis le dispositif 2. Ce traitement comporte des étapes E10 à E18 mémorisées en mémoire 52.

Ce second traitement consiste globalement à effectuer un test sur la valeur du second identificateur morphologique ID2, puis, en fonction du résultat de ce test, à transmettre ou non une table de codage TCE vers le premier dispositif 2. Lorsque le test est négatif, la table de codage TCE n'est pas transmise, et une clé "fictive", par exemple négative, est transmise à sa place.

L'étape E10 est la réception de données codées à l'étape E4, de l'indicateur IN_n représentatif de la table T_n, et de la référence R2, depuis le dispositif 2.

L'étape E11 est la recherche, au moyen de la référence R2, de l'ensemble de tables de codage ETT relatif au dispositif 2 considéré. Ensuite, au moyen de l'indice IN_n, la table T_n est recherchée dans l'ensemble ETT des tables de codage de transmission. La table de codage T_n est ensuite utilisée pour décoder les données codées reçues à l'étape précédente. Le décodage est un décryptage correspondant au cryptage de l'étape E4. L'étape E11 a pour résultat la clé alphanumérique CA, le second identificateur morphologique ID2 et la seconde clé de codage CR de l'utilisateur. Ces données sont mémorisées en mémoire 53.

L'étape suivante E12 est la recherche de la clé alphanumérique CA de l'utilisateur dans la liste mémorisée en mémoire 53. La clé alphanumérique CA permet d'accéder, dans la mémoire 53, aux paramètres relatifs à l'utilisateur concerné, et notamment à l'ensemble ETU de tables de codage de l'utilisateur considéré et à l'identificateur de référence IDR/CR codé par la clé de codage CR.

Si la clé alphanumérique CA n'est pas trouvée en mémoire 53, cela signifie que l'utilisateur n'est pas identifié par le système. En conséquence, le

traitement est terminé et l'utilisateur n'est pas autorisé à effectuer l'opération. Un message d'erreur peut être transmis vers le dispositif 2.

Si la clé alphanumérique CA est trouvée dans la liste mémorisée en mémoire 53, l'étape E12 est suivie par l'étape E13 qui est la recherche, au moyen de la clé de codage CR, de la table TCR dans l'ensemble ETU de tables de codage de l'utilisateur considéré.

L'étape suivante E14 est le codage du second identificateur morphologique ID2 par la table de codage TCR déterminée à l'étape précédente. Cette étape a pour résultat le second identificateur morphologique ID2/CR codé par la clé de codage CR.

L'étape suivante E15 est un test pour déterminer si le second identificateur morphologique ID2/CR codé par la clé de codage CR obtenu à l'étape précédente est identique à l'identificateur de référence IDR/CR codé par la clé de codage CR, mémorisé en mémoire 53. Si la réponse est négative, l'exécution de l'algorithme est terminée.

Si la réponse est positive, l'étape E15 est suivie de l'étape E16 à laquelle est recherchée, au moyen de la clé de codage CE, une table de codage TCE dans l'ensemble ETU de tables de codage de l'utilisateur.

A l'étape suivante E17, une table de codage T_m , avec m entier compris entre 1 et N, est sélectionnée de manière aléatoire parmi l'ensemble ETT de tables de codage de transmission mémorisé en mémoire 53. La table TCE est ensuite codée au moyen de la table T_m.

L'étape suivante E18 est la transmission de la table TCE codée par la table T_m et de l'indice IN_m représentatif de la table T_m, vers le dispositif 2 au moyen du circuit 4.

La **figure 4** représente le traitement effectué par le dispositif 2 lorsqu'il reçoit la table TCE codée par la table T_m et l'indicateur IN_m de la table T_m. Ce traitement comporte des étapes E20 à E23 mémorisées en mémoire 25.

Ce troisième traitement consiste globalement à effectuer un test sur la valeur du premier identificateur morphologique ID1/CE codé par la première clé de codage CE.

L'étape E20 est la réception de la table TCE codée par la table T_m et de l'indice de la table T_m.

L'étape suivante E21 est le décodage de la table TCE en utilisant la table T_m. Pour cela, l'indicateur IN_m permet tout d'abord de retrouver la table T_m dans l'ensemble ETT de tables de codage de tramsmission, puis la table T_m est utilisée pour un décryptage de la table TCE correspondant au cryptage de l'étape E17.

L'étape suivante E22 est le codage de l'identificateur morphologique ID1 au moyen de la table TCE. Cette étape a pour résultat l'identificateur morphologique ID1/CE codé par la clé CE.

L'étape suivante est un test pour déterminer si l'identificateur morphologique ID1/CE codé par la clé CE est égal à l'identificateur de référence IDE/CE codé par la clé CE, mémorisé en mémoire 26 à l'étape E1. Si la réponse est négative, alors l'utilisateur n'est pas autorisé à effectuer l'opération et l'exécution de l'algorithme est terminée.

Si la réponse est positive, alors l'authentification de l'utilisateur est terminée. L'opération qu'il souhaite accomplir est alors autorisée. Il est alors possible de passer à cette opération proprement dite.

Les applications de la présente invention sont notamment :

- les retraits d'argent par carte bancaire dans une billetterie,
- les transactions commerciales impliquant un paiement par carte bancaire, par exemple via le réseau Internet,
- l'accès de personne à un local, ou à un véhicule,
- l'accès aux données d'un serveur informatique, via un réseau public ou privé.

Bien entendu, la présente invention n'est nullement limitée aux modes de réalisation décrits et représentés, mais englobe, bien au contraire, toute variante à la portée de l'homme du métier.

REVENDICATIONS

1. Procédé d'authentification d'un utilisateur, utilisant une source (1) de données propres à l'utilisateur, et un premier et un second dispositifs (2,5) de traitement,

caractérisé en ce qu'il comporte les étapes de :

- formation (E2, E3) d'un premier et d'un second identificateurs morphologiques (ID1, ID2), par le premier dispositif (2),
- lecture (E1) d'un premier identificateur de référence (IDE/CE) codé par une première clé de codage (CE), mémorisé dans la source de données (1), par le premier dispositif (2),
- lecture (E1) d'une seconde clé de codage (CR) mémorisée dans la source de données (1), par le premier dispositif (2),
- transmission (E5) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) au second dispositif (5),
- codage (E14) du second identificateur morphologique (ID2) par la seconde clé de codage (CR), par le second dispositif (5),
- comparaison (E15), par le second dispositif, du second identificateur morphologique (ID2/CR) codé par la seconde clé de codage avec un second identificateur de référence (IDR/CR) codé par la seconde clé de codage et mémorisé dans le second dispositif (5) et, si il y a identité,
- transmission (E18) d'une première table de codage (TCE), mémorisée dans le second dispositif (5), vers le premier dispositif (2),
- codage (E22) du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE), par le premier dispositif (2),
- comparaison (E23), par le premier dispositif (2), du premier identificateur morphologique (ID1/CE) codé au moyen de la première table de codage avec le premier identificateur de référence (IDE/CE) codé par la première clé de codage.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que l'étape de formation comporte la lecture (E2) d'un identificateur morphologique initial (ID) puis le partage de l'identificateur morphologique initial en les premier et second identificateurs morphologiques (ID1, ID2).

3. Procédé d'authentification selon la revendication 1 ou 2, caractérisé en ce que l'étape de transmission du second identificateur morphologique et de la seconde clé de codage au second dispositif comporte (E4) la sélection d'une première table de codage de transmission (T_n) dans un ensemble de table de codage de transmission, le codage du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) par la première table de codage de transmission, et la transmission (E5) du second identificateur morphologique et de la seconde clé de codage codés par la première table de codage de transmission.

4. Procédé d'authentification selon la revendication 3, caractérisé en ce qu'il comporte l'étape de décodage (E11), par le second dispositif (5), du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) codés par la première table de codage de transmission, préalablement à l'étape de codage (E14) du second identificateur morphologique (ID2) par la seconde clé de codage (CR).

5. Procédé d'authentification selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comporte en outre la lecture (E1) d'une clé alphanumérique (CA), mémorisée dans la source de données (1), par le premier dispositif (2), et la transmission (E5) de la clé alphanumérique (CA) au second dispositif (5).

6. Procédé d'authentification selon les revendications 3 et 5, caractérisé en ce qu'il comporte le codage (E4), par le premier dispositif (2), de la clé alphanumérique (CA) par la première table de codage de transmission (T_n), préalablement à sa transmission (E5).

7. Procédé d'authentification selon la revendication 6, caractérisé en ce qu'il comporte le décodage (E11), par le second dispositif (5), de la clé alphanumérique codée par la première table de codage de transmission.

8. Procédé d'authentification selon l'une quelconque des revendications 5 à 7, caractérisé en ce que la clé alphanumérique (CA) permet d'accéder (E13) à un ensemble de table de codage (ETU) mémorisé dans le second dispositif (5), et en ce que la seconde clé de codage (CR) permet de trouver une seconde table de codage (TCR) dans cet ensemble de codage.

9. Procédé d'authentification selon l'une quelconque des revendications 5 à 8, caractérisé en ce que la clé alphanumérique (CA) permet d'accéder (E13) au second identificateur de référence codé par la seconde clé de codage (IDR/CR), mémorisé dans le second dispositif (5).

10. Procédé d'authentification selon l'une quelconque des revendications 1 à 9, caractérisé en ce que la transmission (E18) de la première table de codage (TCE) comporte le codage préalable (E17), par le second dispositif (5), de la première table de codage par une seconde table de codage de transmission (T_m).

11. Procédé d'authentification selon la revendication 10, caractérisé en ce qu'il comporte le décodage (E21), par le premier dispositif (2), de la première table de codage (TCE) codée par la seconde table de codage de transmission, préalablement au codage (E22) du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE).

12. Système d'authentification d'un utilisateur, comportant une source (1) de données propres à l'utilisateur, et un premier et un second dispositifs (2,5) de traitement,

caractérisé en ce que le premier dispositif (2) comporte :

- des moyens de formation (23) d'un premier et d'un second identificateurs morphologiques (ID1, ID2),

- des moyens de lecture (21) d'un premier identificateur de référence (IDE/CE) codé par une première clé de codage (CE), mémorisé dans la source de données (1),

- des moyens de lecture (21) d'une seconde clé de codage (CR) mémorisée dans la source de données (1),

- des moyens de transmission (3) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) au second dispositif (5),

en ce que le second dispositif (5) comporte :

- des moyens de codage (51) du second identificateur morphologique (ID2) par la seconde clé de codage (CR),

- des moyens de comparaison (51) du second identificateur morphologique (ID2/CR) codé par la seconde clé de codage avec un second identificateur de référence (IDR/CR) codé par la seconde clé de codage et mémorisé dans le second dispositif (5), et,

- des moyens de transmission (4), si il y a identité, d'une première table de codage (TCE), mémorisée dans le second dispositif (5), vers le premier dispositif (2),

et en ce que le premier dispositif (2) comporte :

- des moyens de codage (23) du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE),

- des moyens de comparaison (23) du premier identificateur morphologique (ID1/CE) codé au moyen de la première table de codage avec le premier identificateur de référence (IDE/CE) codé par la première clé de codage.

13. Système d'authentification selon la revendication 12, caractérisé en ce que le premier dispositif (2) comporte des moyens de lecture (21) d'un identificateur morphologique initial (ID) et des moyens de partage (23) de

l'identificateur morphologique initial en les premier et second identificateurs morphologiques (ID1, ID2).

14. Système d'authentification selon la revendication 12 ou 13, caractérisé en ce que le premier dispositif (2) comporte :

- des moyens de mémorisation d'un ensemble de table de codage de transmission,

- des moyens de sélection (23) d'une première table de codage de transmission (T_n) dans l'ensemble de table de codage de transmission,

- des moyens de codage (23) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) par la première table de codage de transmission, et

- des moyens de transmission (3) du second identificateur morphologique et de la seconde clé de codage codés par la première table de codage de transmission.

15. Système d'authentification selon la revendication 14, caractérisé en ce que le second dispositif (5) comporte des moyens de décodage (51) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) codés par la première table de codage de transmission, préalablement au codage du second identificateur morphologique (ID2) par la seconde clé de codage (CR).

16. Système d'authentification selon l'une quelconque des revendications 12 à 15, caractérisé en ce que le premier dispositif (2) comporte en outre des moyens de lecture (21) d'une clé alphanumérique (CA), mémorisée dans la source de données (1), et des moyens de transmission (3) de la clé alphanumérique (CA) au second dispositif (5).

17. Système d'authentification selon les revendications 14 et 16, caractérisé en ce que le premier dispositif (2) comporte des moyens de codage

(23) de la clé alphanumérique (CA) par la première table de codage de transmission (T_n), préalablement à sa transmission.

18. Système d'authentification selon la revendication 17, caractérisé en ce que le second dispositif (5) comporte des moyens de décodage (51) de la clé alphanumérique codée par la première table de codage de transmission.

19. Système d'authentification selon l'une quelconque des revendications 16 à 18, caractérisé en ce que le second dispositif (5) comporte des moyens de mémorisation (53) d'un ensemble de table de codage (ETU), en ce que la clé alphanumérique (CA) permet d'accéder (E13) à l'ensemble de table de codage (ETU), et en ce que la seconde clé de codage (CR) permet de trouver une seconde table de codage (TCR) dans cet ensemble de codage.

20. Système d'authentification selon l'une quelconque des revendications 16 à 19, caractérisé en ce que la clé alphanumérique (CA) permet d'accéder (E13) au second identificateur de référence codé par la seconde clé de codage (IDR/CR), mémorisé dans le second dispositif (5).

21. Système d'authentification selon l'une quelconque des revendications 12 à 20, caractérisé en ce que le second dispositif (5) comporte des moyens de codage (51) de la première table de codage par une seconde table de codage de transmission (T_m) préalablement à la transmission de la première table de codage (TCE).

22. Système d'authentification selon la revendication 21, caractérisé en ce que le premier dispositif (2) comporte des moyens de décodage (23) de la première table de codage (TCE) codée par la seconde table de codage de transmission, préalablement au codage du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE).

23. Dispositif (2) de traitement de données pour authentifier un utilisateur, adapté à échanger des données avec un autre dispositif (5),

caractérisé en ce qu'il comporte :

- des moyens de formation (23) d'un premier et d'un second identificateurs morphologiques (ID1, ID2),

- des moyens de lecture (21) d'un premier identificateur de référence (IDE/CE) codé par une première clé de codage (CE), mémorisé dans une source de données (1),

- des moyens de lecture (21) d'une seconde clé de codage (CR) mémorisée dans la source de données (1),

- des moyens de transmission (3) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) à l'autre dispositif (5).

24. Dispositif (2) selon la revendication 23, caractérisé en ce qu'il comporte :

- des moyens de réception (3) d'une première table de codage (TCE) transmise depuis l'autre dispositif (5),

- des moyens de codage (23) du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE),

- des moyens de comparaison (23) du premier identificateur morphologique (ID1/CE) codé au moyen de la première table de codage avec le premier identificateur de référence (IDE/CE) codé par la première clé de codage.

25. Dispositif (2) selon la revendication 23 ou 24, caractérisé en ce qu'il comporte des moyens de lecture (21) d'un identificateur morphologique initial (ID) et des moyens de partage (23) de l'identificateur morphologique initial en les premier et second identificateurs morphologiques (ID1, ID2).

26. Dispositif (2) selon l'une quelconque des revendications 23 à 25, caractérisé en ce qu'il comporte :

- des moyens de mémorisation d'un ensemble de table de codage de transmission,

- des moyens de sélection (23) d'une première table de codage de transmission (T_n) dans l'ensemble de table de codage de transmission,

- des moyens de codage (23) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) par la première table de codage de transmission, et

- des moyens de transmission (3) du second identificateur morphologique et de la seconde clé de codage codés par la première table de codage de transmission.

27. Dispositif (2) selon l'une quelconque des revendications 23 à 26, caractérisé en ce qu'il comporte en outre des moyens de lecture (21) d'une clé alphanumérique (CA), mémorisée dans la source de données (1), et des moyens de transmission (3) de la clé alphanumérique (CA) à l'autre dispositif (5).

28. Dispositif (2) selon les revendications 26 et 27, caractérisé en ce qu'il comporte des moyens de codage (23) de la clé alphanumérique (CA) par la première table de codage de transmission (T_n), préalablement à sa transmission.

29. Dispositif (2) selon la revendication 24, caractérisé en ce qu'il comporte des moyens de décodage (23) de la première table de codage (TCE) codée par une seconde table de codage de transmission (T_m), préalablement au codage du premier identificateur morphologique (ID1) au moyen de la première table de codage (TCE).

30. Dispositif (5) de traitement de données pour authentifier un utilisateur, adapté à échanger des données avec un autre dispositif (2),

caractérisé en ce qu'il comporte :

- des moyens de réception (3) d'un second identificateur morphologique (ID2) et d'une seconde clé de codage (CR) transmis par l'autre dispositif (2),

- des moyens de codage (51) du second identificateur morphologique (ID2) par la seconde clé de codage (CR),

- des moyens de comparaison (51) du second identificateur morphologique (ID2/CR) codé par la seconde clé de codage avec un second identificateur de référence (IDR/CR) codé par la seconde clé de codage et mémorisé dans le dispositif considéré (5), et,

- des moyens de transmission (4), si il y a identité, d'une première table de codage (TCE), mémorisée dans le dispositif considéré (5), vers l'autre dispositif (2).

31. Dispositif (5) selon la revendication 30, caractérisé en ce qu'il comporte des moyens de décodage (51) du second identificateur morphologique (ID2) et de la seconde clé de codage (CR) codés par une première table de codage de transmission (T_n), préalablement au codage du second identificateur morphologique (ID2) par la seconde clé de codage (CR).

32. Dispositif (5) selon la revendication 31, caractérisé en ce qu'il comporte des moyens de réception (4) d'une clé alphanumérique (CA) codée par la première table de codage de transmission et transmise depuis l'autre dispositif (2), et des moyens de décodage (51) de la clé alphanumérique codée par la première table de codage de transmission.

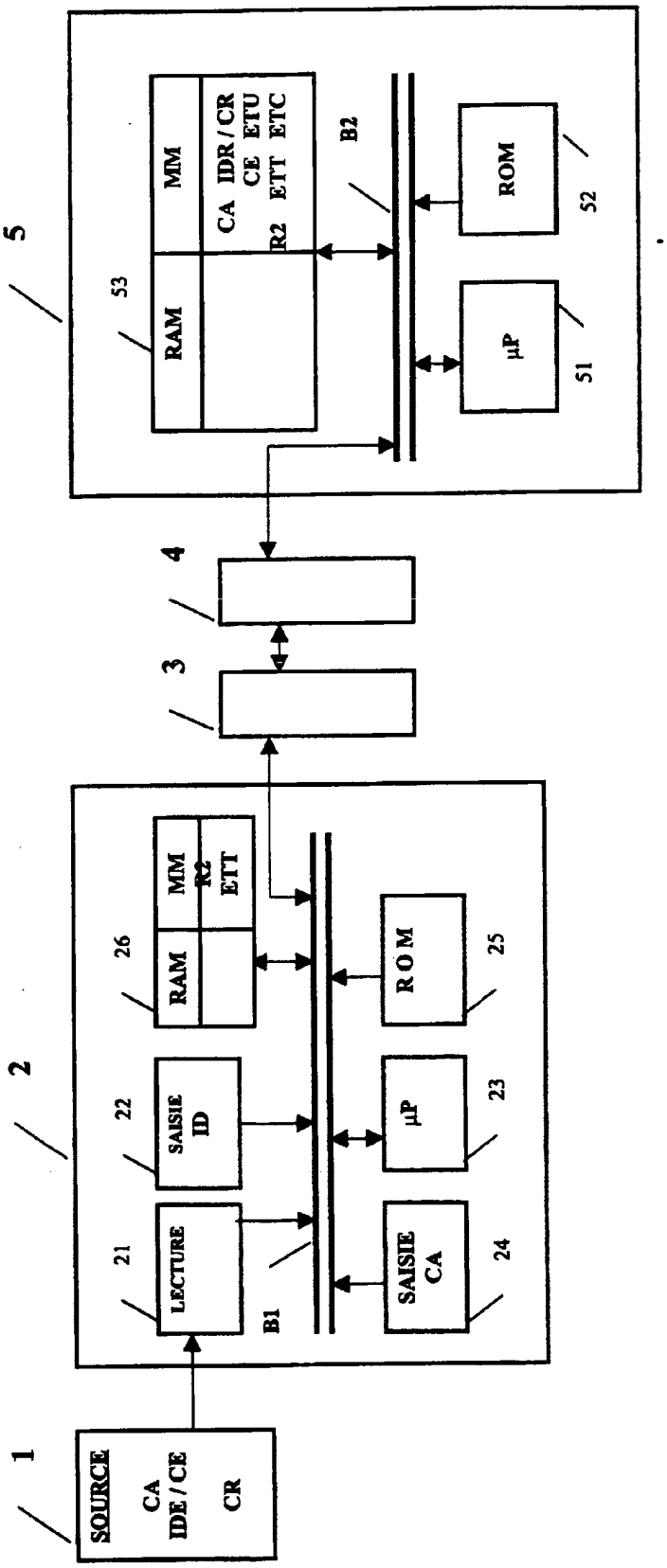
33. Dispositif (5) selon la revendication 32, caractérisé en ce qu'il comporte des moyens de mémorisation (53) d'un ensemble de table de codage (ETU), en ce que la clé alphanumérique (CA) permet d'accéder (E13) à l'ensemble de table de codage (ETU), et en ce que la seconde clé de codage (CR) permet de trouver une seconde table de codage (TCR) dans cet ensemble de codage.

34. Dispositif (5) selon l'une quelconque des revendications 32 à 33, caractérisé en ce que la clé alphanumérique (CA) permet d'accéder (E13) au second identificateur de référence codé par la seconde clé de codage (IDR/CR), mémorisé dans le dispositif considéré (5).

35. Dispositif (5) selon l'une quelconque des revendications 30 à 34, caractérisé en ce qu'il comporte des moyens de codage (51) de la première table de codage (TCE) par une seconde table de codage de transmission (T_m) préalablement à la transmission de la première table de codage (TCE).

2780797

FIG.1



2780797

FIG. 2

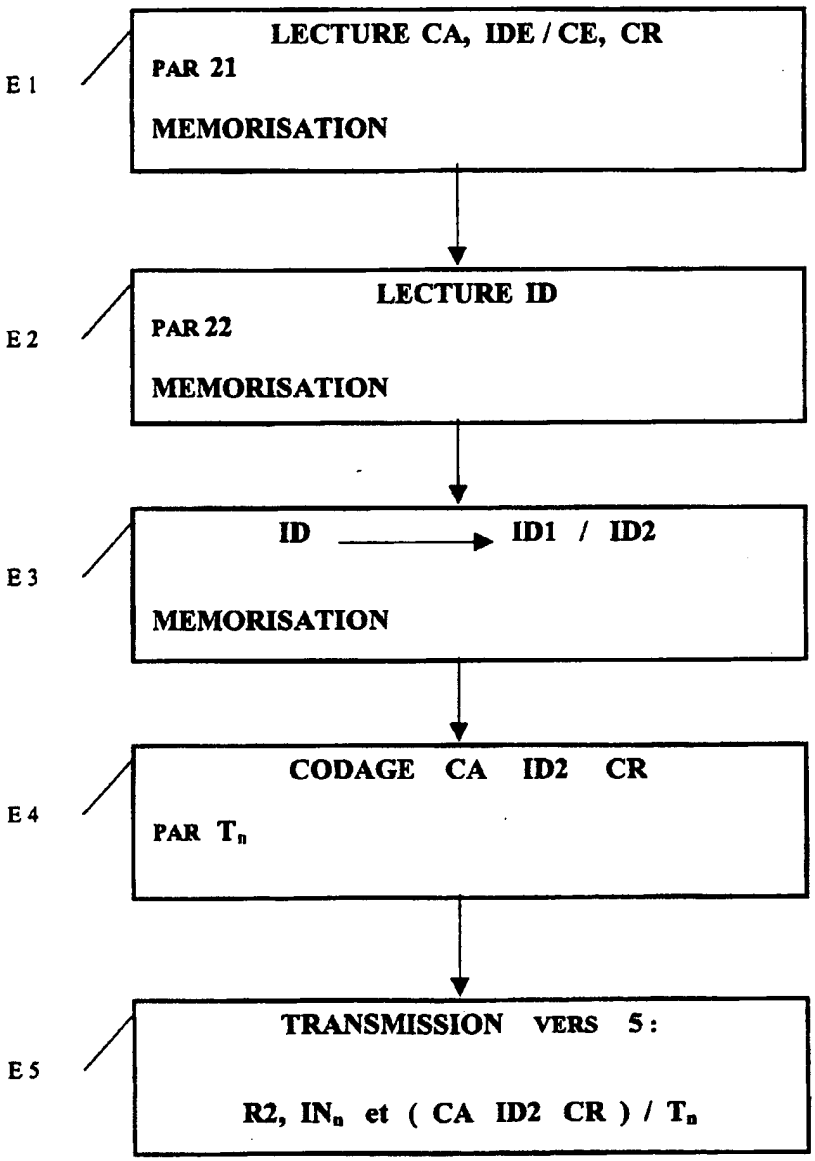


FIG. 3

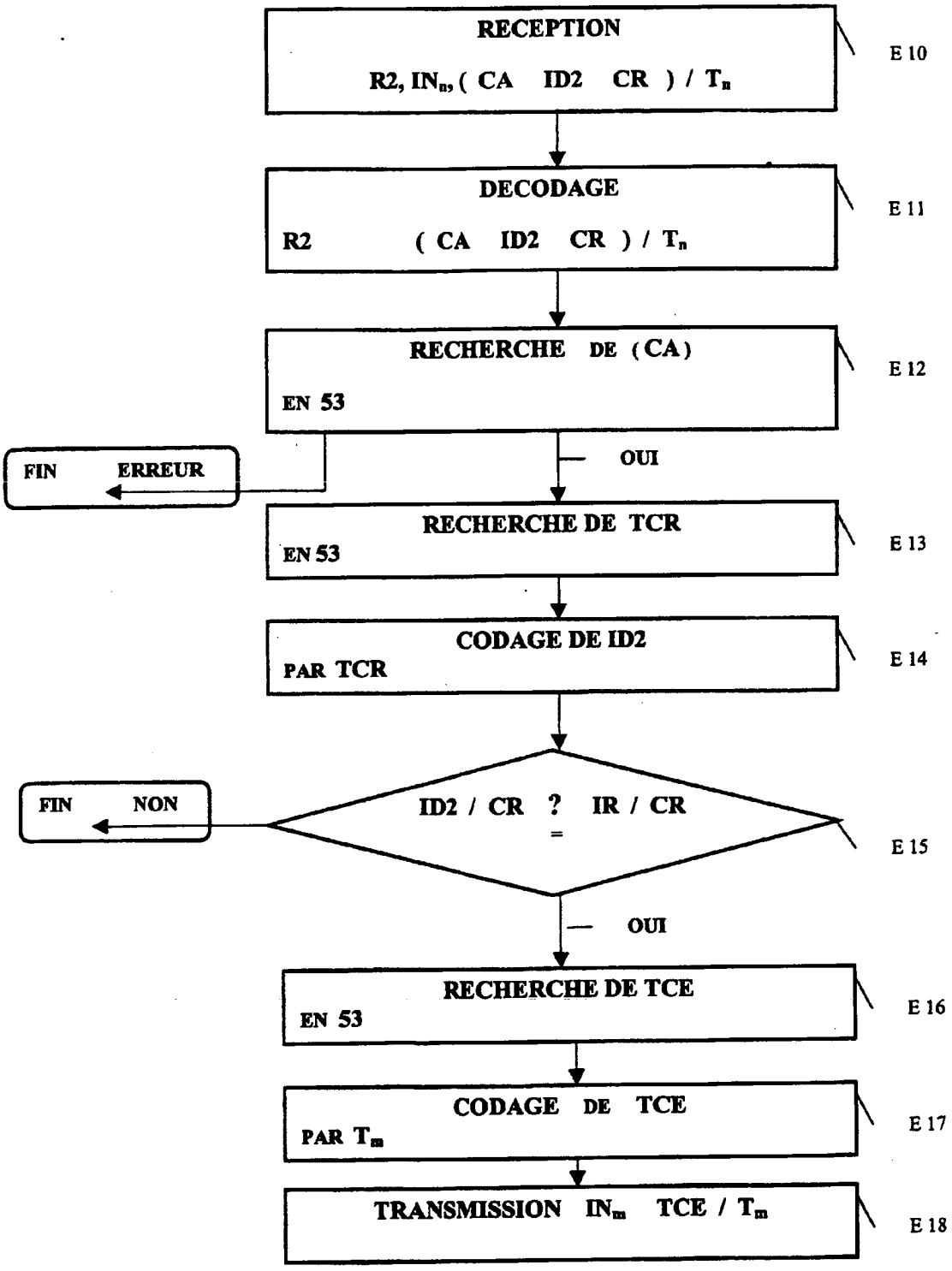
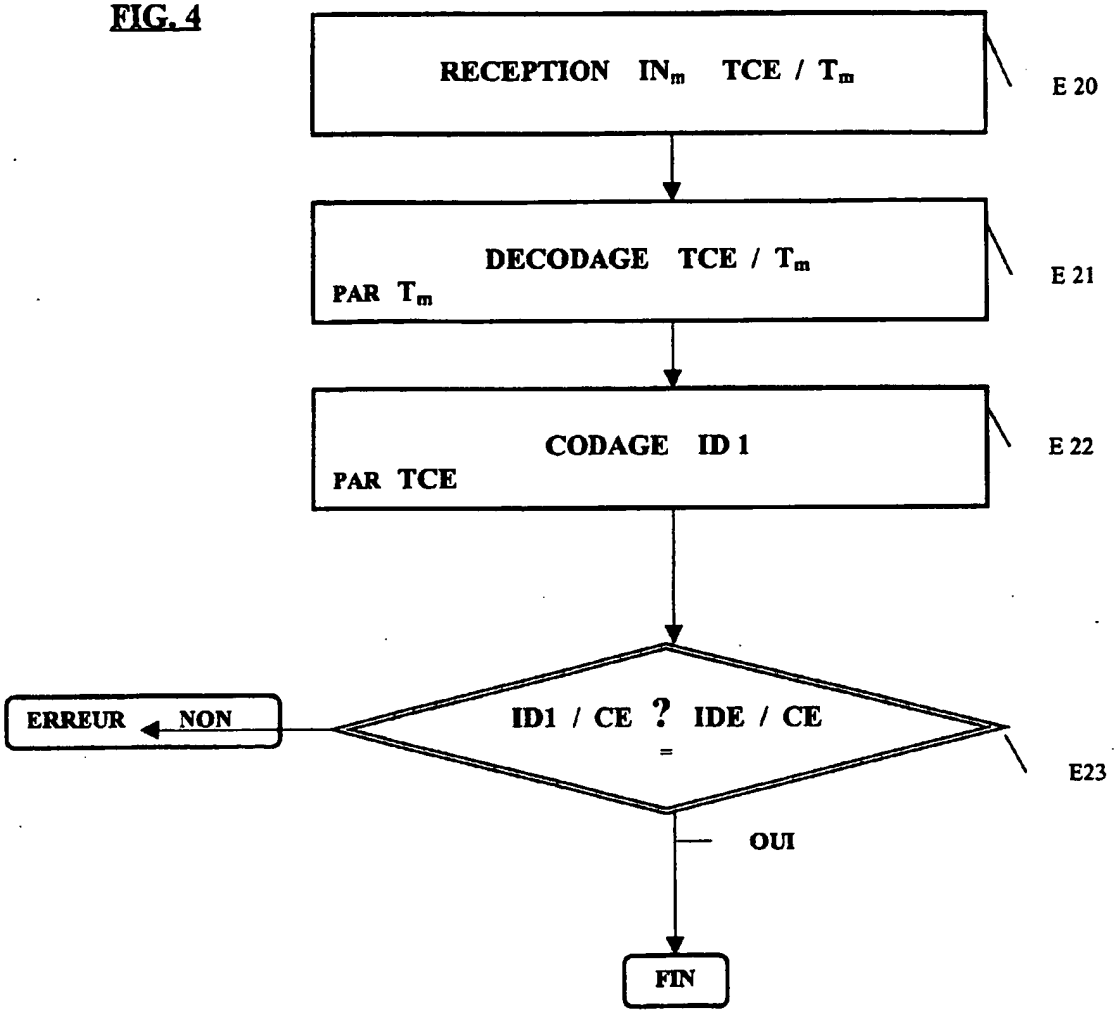

RECEPTION
R2, IN$_n$, (CA ID2 CR) / T$_n$
E 10
DECODAGE
R2 (CA ID2 CR) / T$_n$
E 11
RECHERCHE DE (CA)
EN 53
E 12
FIN ERREUR
OUI
RECHERCHE DE TCR
EN 53
E 13
CODAGE DE ID2
PAR TCR
E 14
FIN NON
ID2 / CR = IR / CR ?
E 15
OUI
RECHERCHE DE TCE
EN 53
E 16
CODAGE DE TCE
PAR T$_m$
E 17
TRANSMISSION IN$_m$ TCE / T$_m$
E 18

FIG. 4


RECEPTION IN_m TCE / T_m
E 20
DECODAGE TCE / T_m
PAR T_m
E 21
CODAGE ID 1
PAR TCE
E 22
ID1 / CE ? IDE / CE
=
E23
ERREUR
NON
OUI
FIN

REPUBLIQUE FRANÇAISE

2780797

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 564644
FR 9808532

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	WO 98 01820 A (DYNAMIC DATA SYSTEMS PTY LTD ;ELBAUM HECTOR DANIEL (AU)) 15 janvier 1998 * abrégé * * page 2, ligne 23 - page 10, ligne 20 * * page 17, ligne 11 - page 19, ligne 4 *	1,12,14, 23,24, 26,30
A	US 4 023 013 A (KINKER DONALD E) 10 mai 1977 * abrégé * * colonne 2, ligne 54 - colonne 3, ligne 5 * * colonne 5, ligne 31 - colonne 6, ligne 42 *	2,13,25
A	US 4 993 068 A (PIOSENKA GERALD V ET AL) 12 février 1991 * colonne 2, ligne 58 - colonne 6, ligne 54; figures 1,2 *	1
A	WO 96 18169 A (KRETZSCHMAR LOREN ;DAVIS VICTORIA (US)) 13 juin 1996 * abrégé * * page 4, ligne 11 - page 8, ligne 15 *	1
A	US 4 605 820 A (CAMPBELL JR CARL M) 12 août 1986	
A	GB 2 227 111 A (TOKYO SHIBAURA ELECTRIC CO) 18 juillet 1990	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G07C
G06K
H04L
G07F

1

Date d'achèvement de la recherche	Examinateur
14 avril 1999	Bocage, S

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publiéqu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

7 / 11 WPAT - ©Thomson Derwent - image
AN - 2000-173807 [16]
XP - N2000-129427
TI - Method of user authentication for banking, payment or access control
DC - T01 T05 W01
PA - (BONN/) BONNET G
(FRAN/) FRANCOIS P
IN - BONNET G; FRANCOIS P
NP - 1
NC - 1
PN - FR2780797 A1 20000107 DW2000-16 G06F-012/14 30p *
AP: 1998FR-0008532 19980703
PR - 1998FR-0008532 19980703
IC - G06F-012/14 H04L-009/14
AB - FR2780797 A
NOVELTY - The authentication forms two morphological identifications (ID1 , ID2), an identifier reference encrypted with a first key (CE), and a second key (CR). The second identifier (ID2) and key are used by a second device (5), to create then return an encoding table. The first device (2) encrypts the first identifier (ID1) with the encoding table to compare with the encrypted first reference code.
USE - Access control to financial services or to locations or facilities
ADVANTAGE - Improved reliability of authentication of users, reducing risk of fraudulent access.
DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of the system
morphological identifications ID1,ID2
First and second encryption keys CE, CR
Receiving device 5
Sending device 2(Dwg.1/4)
MC - EPI: T01-D01 T01-H01C2 T01-J05A1 T01-J12C T05-L02 W01-A05A
UP - 2000-16

SS	Results
1	45452 POLICY OR POLICIES
2	645 ENFORC+ (2D) (RULE? OR POLIC+)
3	1376 ADMINISTRAT+ AND RULE?
4	9 1 AND 2 AND 3
5	61 MORPH+ (3D) USER?
6	227 USER? (2D) (ID? OR IDENTIFIER?)
7	0 5 AND 6
8	8 MORPH+ (2D) (ID? OR IDENTIFIER?)

Search statement 9

SS	Results	
1	50	MORPH+ (3D) USER?
2	2691	USER? (2D) (ID? OR IDENTIFIER?)
3	0	1 AND 2
4	11	MORPH+ (2D) (ID? OR IDENTIFIER?)
5	2	SWAP+ (2D) (ID? OR IDENTIFIER?)
6	37	USER? (2D) CREDENTIAL?
7	5	2 AND 6